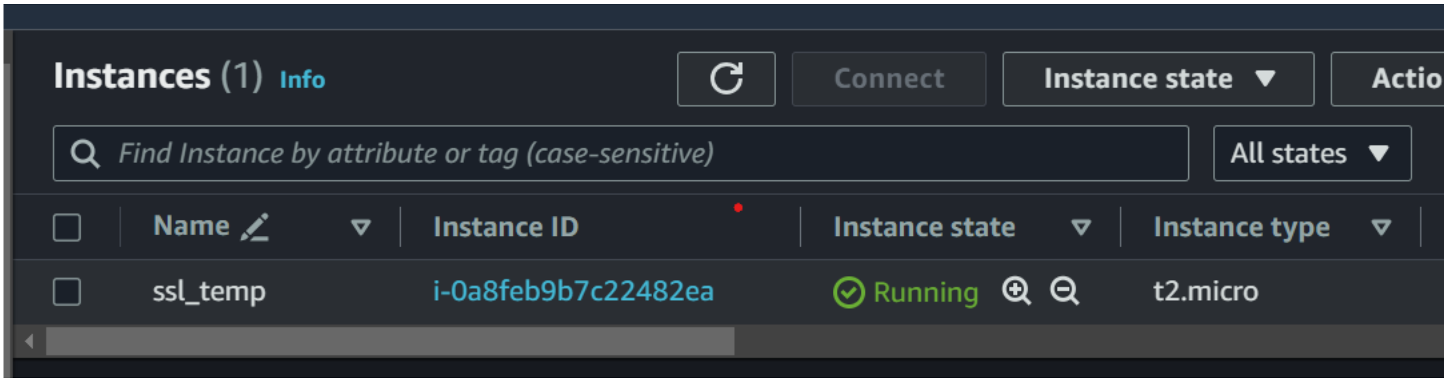
AWS DOCUMENTATION

SSL Certificate

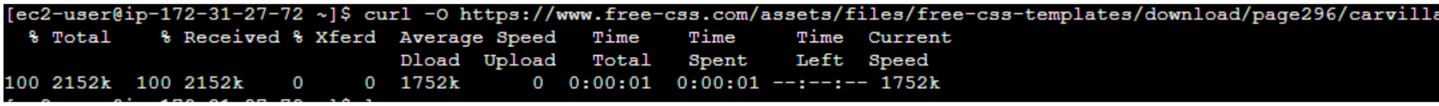
Step I : Create the Instance.



□	Name	Instance ID	Instance state	Instance type
□	ssl_temp	i-0a8feb9b7c22482ea	Running	t2.micro

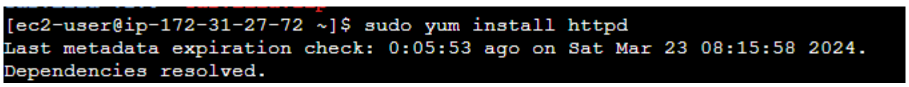
Step II : go to browser and copy the link address for downloading free template then connect Instance and download it.

Step III : then Unzip it.

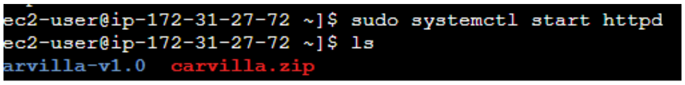


```
[ec2-user@ip-172-31-27-72 ~]$ curl -O https://www.free-css.com/assets/files/free-css-templates/download/page296/carvilla
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 2152k  100 2152k    0     0  1752k      0  0:00:01  0:00:01 --:--:-- 1752k
```

Step IV : Install the httpd ,start it.

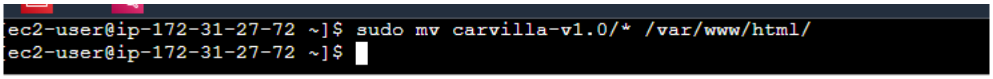


```
[ec2-user@ip-172-31-27-72 ~]$ sudo yum install httpd
Last metadata expiration check: 0:05:53 ago on Sat Mar 23 08:15:58 2024.
Dependencies resolved.
```



```
ec2-user@ip-172-31-27-72 ~]$ sudo systemctl start httpd
ec2-user@ip-172-31-27-72 ~]$ ls
arvilla-v1.0  carvilla.zip
```

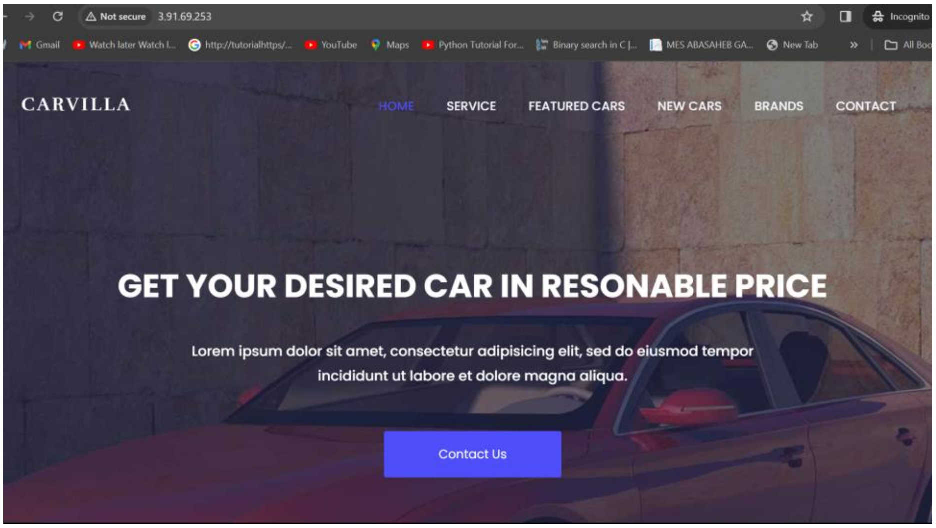
Step V : move the template file in /var/www/html/



```
[ec2-user@ip-172-31-27-72 ~]$ sudo mv carvilla-v1.0/* /var/www/html/
[ec2-user@ip-172-31-27-72 ~]$ 
```

Step VI : Copy the Instance IP and Paste it in another browser.

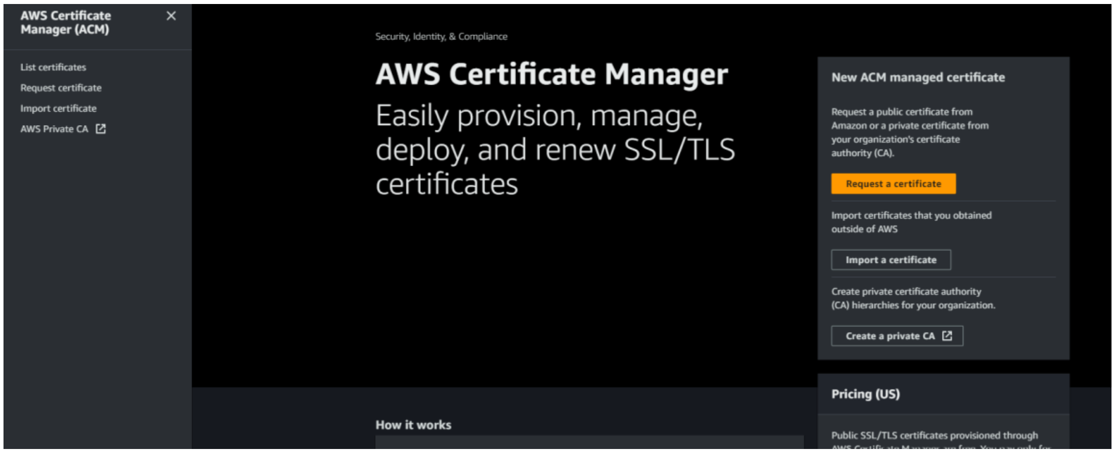
Step VII : See here, the hosted page properly but it is not secure.



GET YOUR DESIRED CAR IN RESONABLE PRICE

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Step VIII : go to certificate manager page, click on request a certificate.



AWS Certificate Manager

Easily provision, manage, deploy, and renew SSL/TLS certificates

New ACM managed certificate

Request a public certificate from Amazon or a private certificate from your organization's certificate authority (CA).

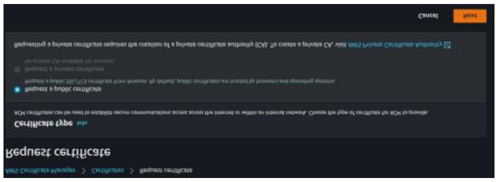
Import certificates that you obtained outside of AWS

Create private certificate authority (CA) hierarchies for your organization.

Pricing (US)

Public SSL/TLS certificates provisioned through

Step VIII : request a public certificate and click on Next.



AWS Certificate Manager > Certificates > Request certificate

Request certificate

Certificate type Info

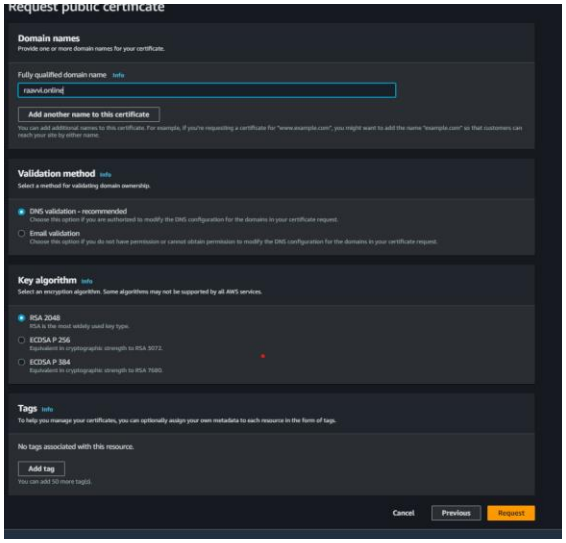
ACM certificates can be used to establish secure communications across the Internet or within an internal network. Choose the type of certificate for ACM to provide.

● Request a public certificate
Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.

○ Request a private certificate
No private CAs available for issuance.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit AWS Private Certificate Authority

Step IX : then give the fully qualified domain name, DNS validation and click on Request.



Request public certificate

Domain names
Provide one or more domain names for your certificate.

Fully qualified domain name Info
raavvi.online

Add another name to this certificate
You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Validation method Info
Select a method for validating domain ownership.

● DNS validation - recommended
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

○ Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

Key algorithm Info
Select an encryption algorithm. Some algorithms may not be supported by all AWS services.

● RSA 2048
RSA is the most widely used key type.

○ ECDSA P 256
Equivalent in cryptographic strength to RSA 3072.

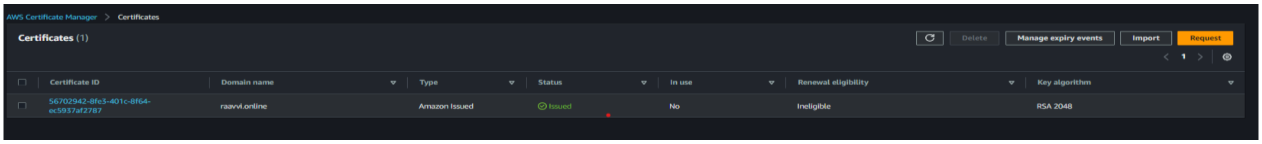
○ ECDSA P 384
Equivalent in cryptographic strength to RSA 7680.

Tags Info
To help you manage your certificates, you can optionally assign your own metadata to each resource in the form of tags.

No tags associated with this resource.

Add tag
You can add 50 more tag(s).

Step X : see here ,Status is Issued.

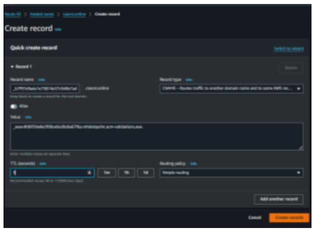


AWS Certificate Manager > Certificates

Certificates (1)

Certificate ID	Domain name	Type	Status	In use	Renewal eligibility	Key algorithm
56702942-8fe3-401c-8f64-ec5937af2787	raavvi.online	Amazon Issued	✓ Issued	No	Ineligible	RSA 2048

Step XI : now, we have to create record for this certificate in route 53.



Route 53 > Hosted zones > raavvi.online > Create record

Create record Info

Quick create record

Record 1

Record name Info: [illegible] .raavvi.online

Record type Info: CNAME – Routes traffic to another domain name and to some AWS res...

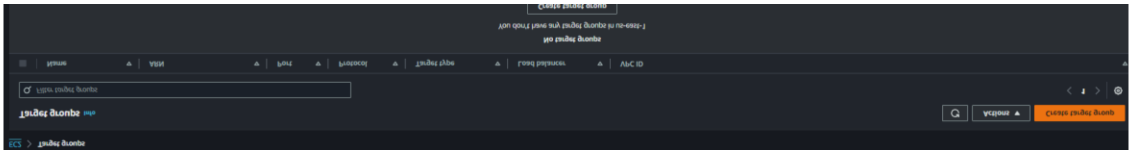
Alias

Value Info: [illegible].acm-validations.aws.

TTL (seconds) Info

Routing policy Info: Simple routing

Step XII : then, go to EC2 service and click on create Target group.



ECS > Target groups

Target groups Info

Actions ▲ | Create target group

Filter target groups

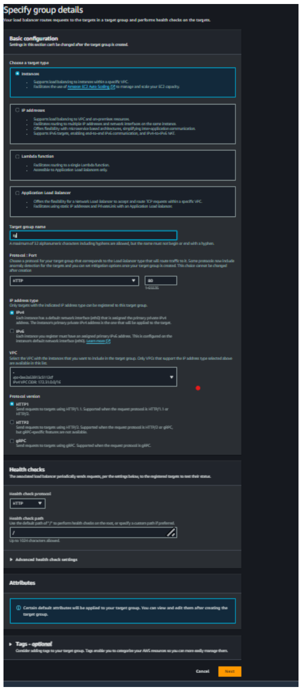
Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID

No target groups

You don't have any target groups in us-east-1

Create target group

Step XIII : give the name and click on next.



Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

● Instances
- Supports load balancing to instances within a specific VPC.
- Facilitates the use of Amazon EC2 Auto Scaling to manage and scale your EC2 capacity.

○ IP addresses
- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

○ Lambda function
- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

○ Application Load Balancer
- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

tg

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation.

HTTP ▾ | 80

1-65535

IP address type

Only targets with the indicated IP address type can be registered to this target group.

● IPv4
Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

○ IPv6
Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). Learn more

VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

-
vpc-0ee2a53913c3112cf
IPv4 VPC CIDR: 172.31.0.0/16

Protocol version

● HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

○ HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

○ gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTP ▾

Health check path

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/

Up to 1024 characters allowed.

▶ Advanced health check settings

Attributes

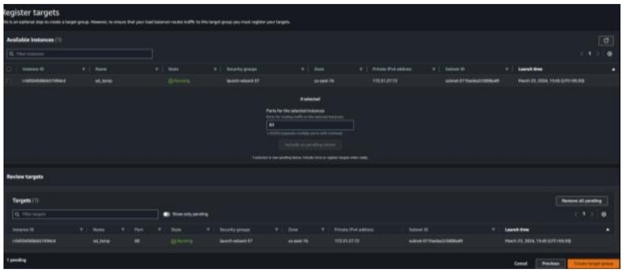
Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

▶ Tags - optional

Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Cancel | Next

Step XIV : register target, review target and and click on create Target group.



Register targets

Available instances (1)

Review targets

Targets (1)

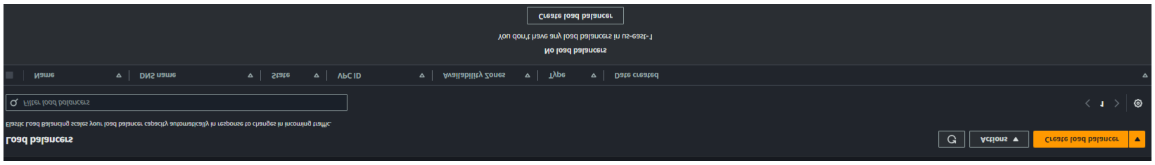
Show only pending

Remove all pending

1 pending

Cancel | Previous | Create target group

Step XV : then click on create Load balancer.



Load balancers

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Actions ▲ | Create load balancer ▲

Filter load balancers

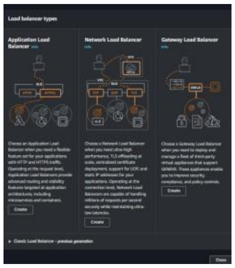
Name	DNS name	State	VPC ID	Availability Zones	Type	Date created

No load balancers

You don't have any load balancers in us-east-1

Create load balancer

Step XVI : then create application Load balancer.



Load balancer types

Application Load Balancer Info

Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.

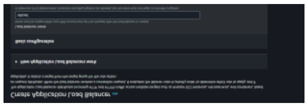
Network Load Balancer Info

Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.

Gateway Load Balancer Info

Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.

Step XVII : give the name to load balancer.



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

▸ How Application Load Balancers work

Basic configuration

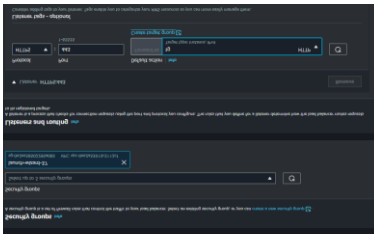
Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

[illegible]

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Step XVIII: then select the security group and add listener HTTPS and select target group.



Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can create a new security group.

Security groups

Select up to 5 security groups ▾

launch-wizard-57 ✕

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▾ Listener HTTPS:443 Remove

Protocol: HTTPS ▾

Port: 443 (1-65535)

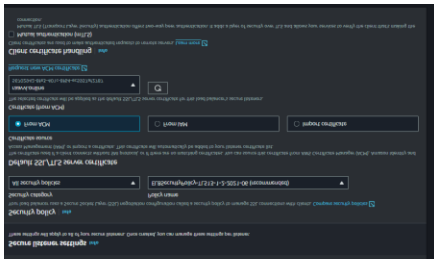
Default action Info: Forward to tg HTTP ▾ (Target type: Instance, IPv4)

Create target group

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Step XIX : then fill the details of Security Policy.



Secure listener settings Info

These settings will apply to all of your secure listeners. Once created, you can manage these settings per listener.

Security policy Info

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. Compare security policies

Security category: All security policies ▾

Policy name: ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended) ▾

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

● From ACM ○ From IAM ○ Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

raavi.online ▾

Request new ACM certificate

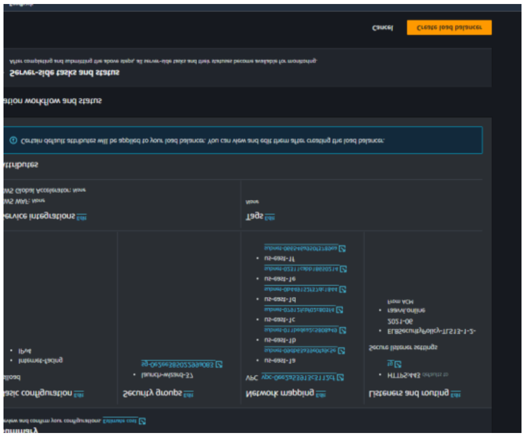
Client certificate handling Info

Client certificates are used to make authenticated requests to remote servers. Learn more

□ Mutual authentication (mTLS)

Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

Step XX : And click on Create Load Balancer.



Summary

Review and confirm your configurations. Estimate cost

Basic configuration Edit
ssload
- Internet-facing
- IPv4

Security groups Edit
- launch-wizard-37

Network mapping Edit
VPC vpc-0ee2a53913c3112cf
- us-east-1a
- us-east-1b
- us-east-1c
- us-east-1d
- us-east-1e
- us-east-1f

Listeners and routing Edit
- HTTPS:443 defaults to tg

Secure listener settings
- ELBSecurityPolicy-TLS13-1-2-2021-06
- raavvi.online From ACM

Service integrations Edit
AWS WAF: None
AWS Global Accelerator: None

Tags Edit
None

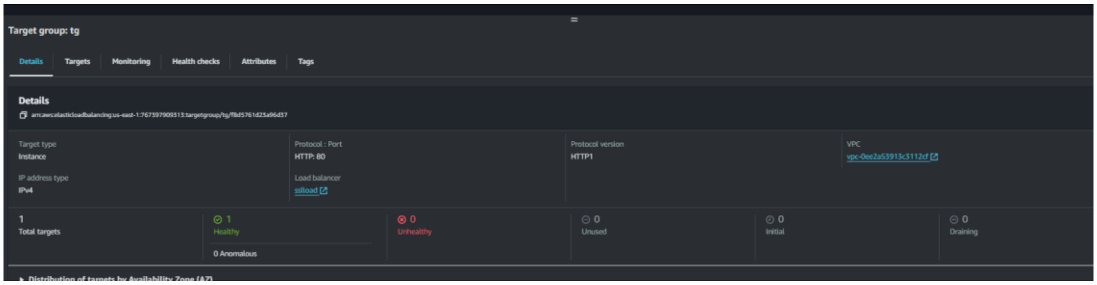
Attributes

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

Creation workflow and status

Server-side tasks and status
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

Step XXI : see here , after connect the load balancer to target group it is healthy now.



Target group: tg

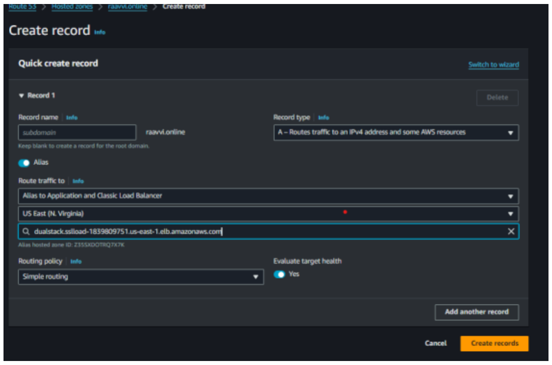
Details
arn:aws:elasticloadbalancing:us-east-1:767397909313:targetgroup/tg/f8d5761d23a96d37

Target type: Instance
IP address type: IPv4
Protocol : Port: HTTP: 80
Load balancer: ssload
Protocol version: HTTP1
VPC: vpc-0ee2a53913c3112cf

1 Total targets
1 Healthy
0 Anomalous
0 Unhealthy
0 Unused
0 Initial
0 Draining

Distribution of targets by Availability Zone (AZ)

Step XXII : then, create record in Route 53 and turn on alias then select alias to Application and Classic Load Balancer, select region.



Route 53 > Hosted zones > raavvi.online > Create record

Create record Info

Quick create record

Record 1

Record name: subdomain raavvi.online
Keep blank to create a record for the root domain.

Record type: A – Routes traffic to an IPv4 address and some AWS resources

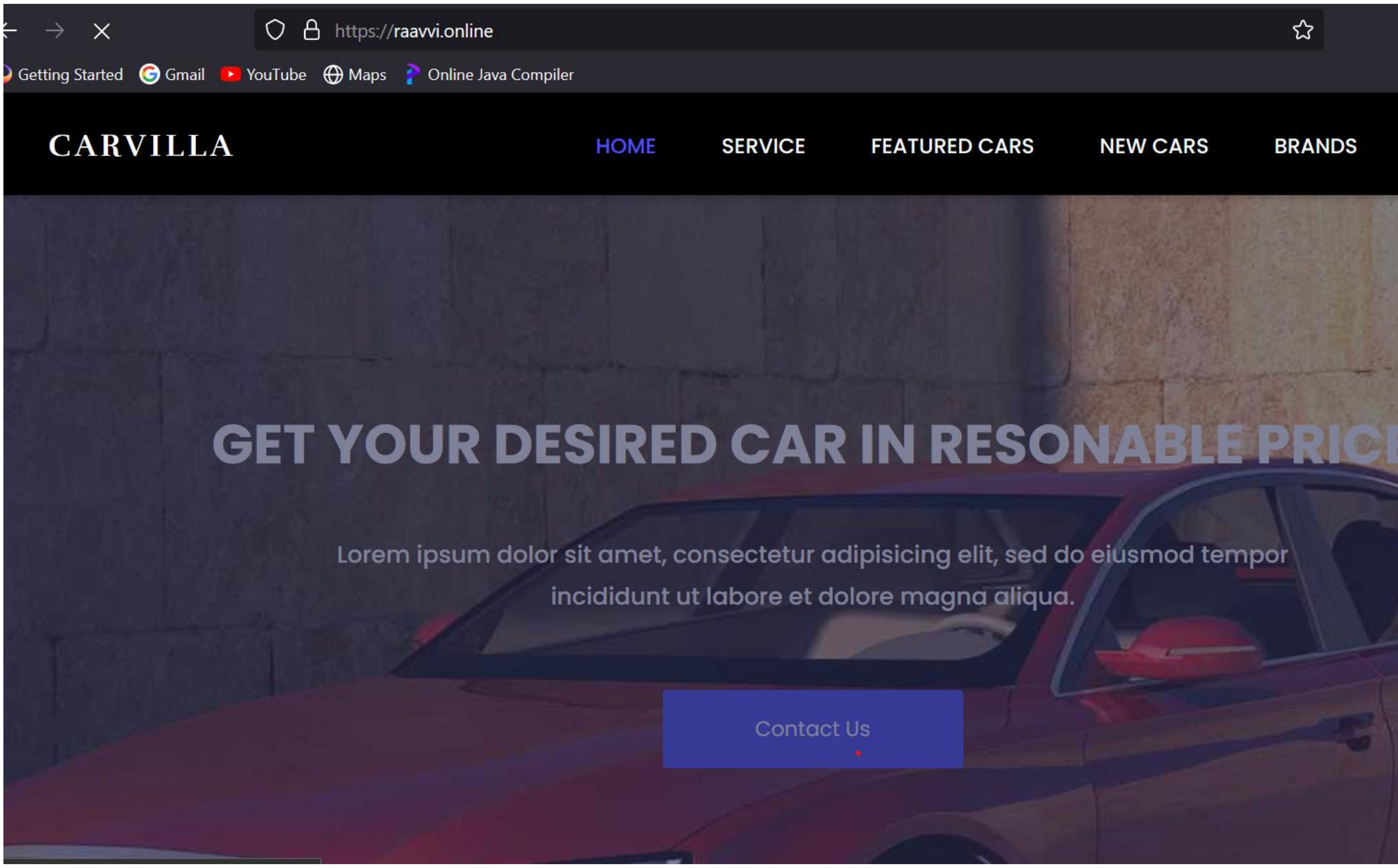
Alias: on

Route traffic to: Alias to Application and Classic Load Balancer
US East (N. Virginia)
dualstack.ssload-1839809751.us-east-1.elb.amazonaws.com
Alias hosted zone ID: Z35SXDOTRQ7X7K

Routing policy: Simple routing

Evaluate target health: Yes

Step XXIII : now hit the domain name in browser and and see here page is secure now.



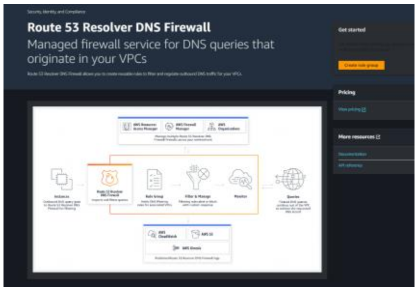
GET YOUR DESIRED CAR IN RESONABLE PRIC

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

DNS SERVICE

Step I : Launch the Instance with adding security rule https .

Step II : then go to Route 53 Service and select the DNS firewall and click on create rule group.

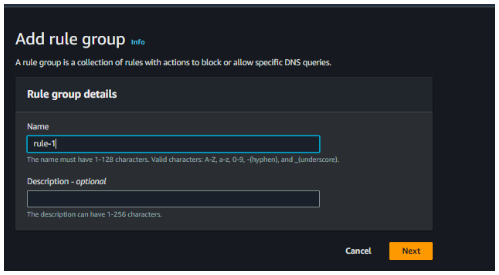


Route 53 Resolver DNS Firewall

Managed firewall service for DNS queries that originate in your VPCs

Route 53 Resolver DNS Firewall allows you to create reusable rules to filter and regulate outbound DNS traffic for your VPCs.

Step III : then add the rule group and click on next.



Add rule group Info

A rule group is a collection of rules with actions to block or allow specific DNS queries.

Rule group details

Name

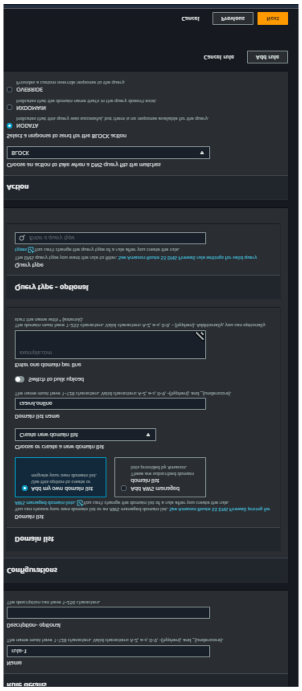
rule-1

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

Description - *optional*

The description can have 1-256 characters.

Step IV : fill the information in group and then In Action choose the BLOCK and click on next.



Rule details

Name

rule-1

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

Description- optional

The description can have 1-256 characters.

Configurations

Domain list

Domain list

You can choose your own domain list or an AWS managed domain list. See Amazon Route 53 DNS Firewall pricing for AWS managed domain lists. You can't change the domain list of a rule after you create the rule.

● Add my own domain list
Use this option to create or migrate your own domain list.

○ Add AWS managed domain list
These are subscribed domain lists provided by Amazon.

Choose or create a new domain list

Create new domain list

Domain list name

raavi.online

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

Switch to bulk upload

Enter one domain per line

example.com

The domain must have 1-255 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen). Additionally, you can optionally start the name with * (asterisk).

Query type - optional

Query type

The DNS query type you want the rule to filter. See Amazon Route 53 DNS Firewall rule settings for valid query types. You can't change the query type of a rule after you create the rule.

Enter a query type

Action

Choose an action to take when a DNS query hits the matches

BLOCK

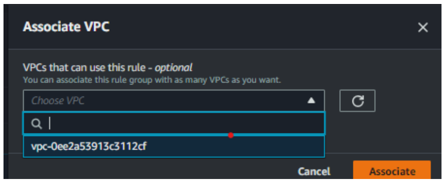
Select a response to send for the BLOCK action

● NODATA
Indicates that this query was successful, but there is no response available for the query.

○ NXDOMAIN
Indicates that the domain name that's in the query doesn't exist.

○ OVERRIDE
Provides a custom override response to the query.

Step V : then associate VPC to group .



Associate VPC

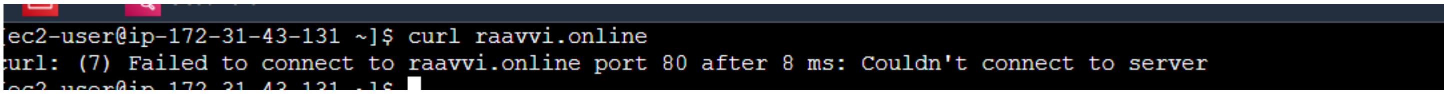
VPCs that can use this rule - *optional*

You can associate this rule group with as many VPCs as you want.

Choose VPC

vpc-0ee2a53913c3112cf

Step VI : then connect the Instance and give command curl “Domain_name”.see here, it showing failed to connect.



```
[ec2-user@ip-172-31-43-131 ~]$ curl raavvi.online
curl: (7) Failed to connect to raavvi.online port 80 after 8 ms: Couldn't connect to server
[ec2-user@ip-172-31-43-131 ~]$
```